Security Requirements for Motor Carriers Transporting Hazardous Materials

RE: Docket No. FMSCA – 02 – 11650 (HM-232A)

Prepared by:
Nicholas V. Sluchevsky
VP Business and Strategic Development
iiMap LLC
(415) 751-1889
Nicholas@iimap.com

1.0 Background.

1.0 Background. This white paper is promulgated in response to a request for information put forth by the Research and Special Projects Agency (RSPA) and the Federal Motor Carrier Safety Administration (FMCSA) of the US Department of Transportation (DoT). Specific reference is made to 49 CFR Part 177, 49 CFR Part 397 <Docket No. FMCSA-02-11650 (HM232A)>.

This paper addresses some of the fundamental requirements for an effective system to insure public safety with regards to the transportation of hazardous materials on US roads. The paper looks only at technology requirements, not regulatory and enforcement issues. Nor is any attempt made to provide an exhaustive review of all available options. The specific areas addressed are:

- Vehicle tracking and monitoring
- Early warning
- Emergency notification

All of the technologies, both hardware and software, discussed here are either, already functioning and available as COTS (commercial, off-the-shelf), or are feasible and deployable within a reasonably short amount of time. No research and development effort is required for an initial deployment.

2.0 Description of problem

2.1 Introduction. In order to insure a comprehensive and effective solution, there are three specific modalities of system operation:

1. Prevention
2. Detection
3. Interception

Prevention includes any solution that would prevent an unauthorized individual from taking over the control of a hazardous materials container. Ideas that are currently in circulation include code locks and biometric scanners. This paper does not address any of the candidate solutions for this problem, except to the extent that the chosen solutions must be capable to working within the larger framework of an effective tracking and early warning system.

Detection refers to the ability of the system to detect whether or not a given vehicle is on its assigned route and whether it presents a credible threat. This is the single most difficult problem to solve and the one that governs the overall effectiveness of the entire system.

Interception includes the capability to the system to alert the appropriate first responders to the existence of a credible threat in a timely manner. In addition, the system must have the capability of remotely shutting down the vehicle. Finally, the system should also have the capability of informing the key decision maker where all responder assets might be located and what the potential targets are.

2.2 Description of problem – System Level. Knowing where a certain mobile asset is located is relatively easy to accomplish with GPS devices. Knowing where many such assets are becomes increasingly difficult. In the present context, 'many' means over 800,000 hazardous materials vehicles daily. Requiring this knowledge in 'real-time' becomes even more difficult.

Simply tracking the location of something does not tell anyone anything useful. What is required is <u>proximity knowledge</u>; in other words, where is that particular vehicle relative to <u>all</u> potential targets? Does the vehicle represent a <u>credible threat?</u> What happens when the 'criticality' or 'vulnerability' of the target changes over a certain period of time, or when intelligence sources suddenly receive credible evidence that a given target has now become a high priority? This set of problems is addressed through techniques that have come to be known as 'geo-fencing'.

In this case, not only has the sheer amount of data to process become enormous – even though the time constraints have remained static – now some of the target information has become dynamic, just like the mobile assets.

Finally, what about tracking locations of likely first responders? This would prove to be of tremendous use for the interception modality, where response time or time to intercept is critical.

The sad truth is that none of the traditional fleet management, tracking, or location based services have this capability.

2.3 Description of the problem – GPS Sensor Level. A different class of problems arises at the GPS service level. The genesis of these problems lies in the fact that the primary focus is on Return on Investment applications, where there is a clear financial benefit to the customer. Because of the highly differentiated sector needs, there exists a considerable amount of customization. In the business world, the focus is not on public safety. Any shift in focus, however slight, in the current legal and regulatory environment, would require a fairly expensive commitment from industry that is already fighting too many regulations.

The problems at the sensor level can generally be summarized as follows:

- Localized solutions with limited ability to integrate with other applications
- Lack of scalability
- Lack of standardization
- Inherent inaccuracies

2.3.1 There are numerous GPS device manufacturers, serving many different markets. In most cases the device and the specific application are tightly coupled and service a specific and narrow market niche. These are localized and customized solutions, addressing a specific customer's needs. The very fact that these solutions are so customized is what has prevented much integration with other applications. It is only necessary to study the GPS service market to realize that there is no single dominant company; this gives a sense of the fragmented nature of this industry.

2.3.2 Directly as a result of the narrowness of GPS service solutions, there is no standard and universal architecture to support the applications. This leads to scalability problems since the applications were not designed with the intent of tracking millions of objects simultaneously.

2.3.3 The localization of GPS solutions implies that they were designed to operate within a clearly defined set of constraints and have little or no need to function with third party applications. Solutions could be engineered that might be optimal for the given conditions, but have no need of operating in a broader, less clearly defined context. Fragmentation of the industry has created fragmentation of solutions, with virtually no standardization.

2.3.4 Finally, GPS services all have inherent inaccuracies, even the new enhanced GPS service. There are several reasons for these inaccuracies, and they are both physical and systemic. Some arise from the physical constraints of the system itself, while others are due to mapping inaccuracies. In business applications, these inaccuracies are not sufficient to be problematic. However, in the case of public safety, the issue becomes much more critical and solutions must be developed to counter the problem. By the very nature of the public safety application, any solutions must be systemic and universal; they cannot be localized.

3.0 Solution. What we propose as an effective solution is a Ground Traffic Control System for all hazardous materials shipments; essentially an analog to the existing Air Traffic Control Systems. Deployment of such a system would be very similar to the ATCS in that there would be regional tracking centers, all linked to a centralized infrastructure. There are several key differences, however, between a GTCS and an ATCS:

- Ability to receive location information from many different GPS services
- Ability to access multiple and distributed databases dynamically
- Ability to notify first responders manually and automatically, as well as remote control applications

Any solution must be looked at on two levels: the architecture and the applications. The architecture is the core technology that binds all of the applications together into a functioning system, much like an operating system in a computer allows multiple office applications to work together.

3.1 Architecture.

In 1994, Executive Order 12906 mandated the creation of the National Spatial Data Infrastructure (NSDI), to be maintained by the Federal Geographic Data Committee. Presumably, the NSDI will be integrated into the Enterprise

Architecture for Homeland Security (EAHS), the spatial data component of which is under the jurisdiction of the National Imagery and Mapping Agency (NIMA).

The proposed concept of a Ground Traffic Control System should heavily utilize the NSDI, although the architecture must be expanded somewhat beyond its scope as purely a data-center to encompass additional requirements, such as sensor inputs, analytics and responder notification.

As part of this expansion of functionality, the following must be mandatory:

1. All component parts should be Web-based and standards based
2. High scalability with very fast response times
3. A distributed architecture
4. Dynamic access of multiple, distributed databases
5. Multi-level security and access rights

3.1.1 **Standards.** In order to achieve a sufficient level of universality, a standard should be mandated whereby any GPS tracking service (fleet management, asset tracking, supply chain management, etc.) will transmit its positioning information to the proposed Ground Traffic Control System using XML (extensible markup language). The use of telecommunications and Internet standards (e.g. J2EE, JDBC compliant, 802.11, http, ftp, etc.) facilitates the ability for a broad range of communications, ranging from low bandwidth devices such as Personal Digital Assistants to high bandwidth file transfers between servers. This will become essential when the system is required to integrate into the EAHS and the NSDI.

3.1.2 **Scalability.** Addressing the problem of scalability is vital in designing an effective public safety application. There are a number of reasons for this:

- The requirement to track up to 1 million hazardous materials shipments daily and determine credible threats to public safety
- The requirement to correlate, in real time, the position of every such shipment relative to all potential targets, as identified by the proposed Dept. of Homeland Security or any other government entity
- The requirement to store all pre-planned routes for hazardous materials shipments and establish adequate geo-fencing for each, as well as responding to real-time re-routing requirements (dynamic routing)
- The probable need for thousands of simultaneous users with different end-user demands
- The requirement to dynamically re-prioritize targets based on current intelligence gathering

The reality of using current GPS and GIS technologies is that none of them can meet these requirements today or in the foreseeable future. Most anyone with GPS capability and a server can design a system to statically track 50, perhaps 100 trucks simultaneously. That is far different from dynamically tracking over 1 million mobile objects and determining the existence of a credible threat to some target. For this purpose a powerful cartographic solution with database drilling capability and a scalable architecture is needed.

3.1.3 **Distributed architecture.** The Internet was conceived as a medium of communications that would survive to some degree even in an all-out nuclear war. Similarly, the architecture of the proposed Ground Traffic Control System, while using the Internet as the primary communications medium, must itself be distributed such that the failure of any one or group of servers providing the backbone must not affect the overall performance. Should failures occur, or should servers be taken off-line for servicing, there should be no appreciable degradation of system performance.

3.1.4 **Dynamic database access.** The reason for requiring a capability to dynamically access multiple and distributed databases is best understood from the decision support perspective. Making critical decisions during the 'fog of war' requires quick and easy access to accurate and relevant information; there is no time to sort through irrelevant material. Unfortunately, the required data may reside in many different locations. Examples might include real-time traffic information, building floor plans, employee records, chemical diffusion studies, radar weather reports, location of all proximate responder assets, etc. The more such information can be accessed from a single-point-of-access, the more effective the system becomes as a decision support tool.

3.1.5 **Security.** The entire system should operate as a Virtual Private Network, taking full advantage of the survivability of the Internet and applying the latest in encryption technology and firewall design. Many levels of access must be accommodated, reflecting the many types of users, ranging from the local agencies and first responders to the intelligence services. Other than credible threat identification and scalability, access control will prove to be the most difficult aspect of building this system.

3.2 **Applications.** The required applications range from data collection, management and display to a variety of analytical solutions. Some applications are required to render solutions in real-time, while others can work off-line. What is common between most of them is the need to share some of the same data; what is common to all is the requirement to serve a common objective, albeit for different classes of users, each with unique requirements.

There are three, distinct classes of applications from the perspective of workflow management:

1. Detection (sensor level)
2. Threat identification (analytics)
3. Communications (reporting and collaboration)

3.2.1 Detection. Within the class of detection applications, there are several modalities, ranging from bio-metric scanners and code-lock systems to geo-fencing. Some of these modalities are active, preventing an action at the point of contact, while others are passive in the sense that they simply forward information on upstream. A code-lock system is active because it requires the driver to enter an activation code to gain access, whereas the geo-fencing applications are passive since they identify a credible threat but then pass the information on to another application. The application does not, by itself, undertake any direct action.

In each of these cases, public safety concerns mandate the applications to make worst-case assumptions at all times. This means that an assumption must be made that every detection modality has been compromised immediately after it's last status report. Multiple modalities do provide a measure of additional security in terms of 'soft-failure', however the final safeguard lies in the capability of the analytics to determine whether a credible threat exists.

3.2.2 Credible threat identification. What, then, is a credible threat? How does a credible threat differ from a non-threat? Any solution with a high false-alarm rate is next to worthless.

There are two ways to establish a credible threat and both must be available:

- Data correlation
- Query

In short, there needs to be a mechanism for comparing all available data and finding clues to possible behavior, as well as a means of directly communicating with the driver, either by voice or some means of electronic messaging.

The critical information required to make a credible threat assessment is as follows:

- Input from all detection modalities
  - (a) Bio-metric scanners
  - (b) Code-lock entry systems
  - (c) Container to tractor matching
  - (d) Geo-fencing
- Present time target vulnerability and criticality assessment
- Other intelligence as available

Any violations of items 1 (a) – (c) are deemed a credible threat automatically and a request for intercept should be triggered. (Container to tractor matching refers to the ability to compare a container's ID code with the both the truck and driver's ID codes.)

As stated earlier, it must be assumed that all of these modalities can be compromised in some way. The last resort is based on analytics and geo-fencing, in effect analyzing a vehicle's behavior to ascertain the existence of a threat.

Geo-fencing requires knowledge of where a given vehicle is at a given time. There are two types of geo-fencing, inclusive and exclusionary. Inclusive geo-fencing refers to a vehicle traveling within some pre-determined area, for instance along an allowable route. Exclusionary geo-fencing refers to a vehicle being restricted from travel within some pre-defined area, for example within 5 miles of a nuclear power plant. Violation of either of these conditions would cause an alert to be sent to the closest tracking center.

Once a vehicle is outfitted with some form of GPS device capable of transmitting its position to the tracking center, both types of geo-fencing can be implemented in software. This should be mandatory since it can easily be demonstrated that reliance on only one or the other will generate too many false alarms. Furthermore, for both consistency and effective operations, there should be only one geo-fencing solution used by the tracking centers – a proliferation of solutions will have disastrous consequences since no two will behave exactly the same way, leading to confusion. Finally, as already mentioned, the solution must be capable of handling the required load, even under worst-case conditions. Such capability currently exists, although not yet in a productized or deployable form.

For geo-fencing to effectively function as a last resort detection and interception application, it must also be mandatory that every trip made by a hazardous materials carrier generate an electronic manifest that is made available to the proposed Ground Traffic Control System. This must apply equally to previously scheduled deliveries, as well as 'hand tag' deliveries, the last minute route changes effected by dispatchers due to some scheduling changes. A review of workflow of hazmat carriers shows that, while this is an inconvenience to some carriers, it is quite minor and not difficult to implement. The application to generate electronic manifests can be easily included in existing workflow with little, if any, behavior change required of the organization.

The purpose of an electronic manifest is to provide the GTCS with an authorized route plan, any deviation from which would result in an alert. This data would be required for any form of inclusive geo-fencing.

Exclusionary geo-fencing requires additional data – a priori knowledge of all, or most, potential targets. Once a potential target is known it is possible to start building exclusion zones around that target and storing these in a database.

In May 2002, the Transportation Policy and Analysis Center of Science Applications International Corporation (SAIC) prepared a report for The American Association of State Highway and Transportation Officials' Security Task Force setting forth a comprehensive methodology for critical asset identification and protection. Essentially, this report outlines an algorithmic approach to determining a given asset's vulnerability (to attack) and criticality (consequences if attacked). This allows someone to create a priority matrix that can be stored in the targets' database. Furthermore, this methodology envisages a process whereby this data can be dynamically updated, pursuant to new intelligence findings. This is a powerful tool that should be standardized and mandated immediately.

3.2.3 **Data aggregation.** Once an alert is received by the responsible tracking facility, additional data may be required for adequate decision support. This data may reside in many different locations, under control of different public and private organizations. As previously mentioned, the National Spatial Data Infrastructure is ultimately responsible for assembling all spatial data under government jurisdiction. This, alone, may be a nearly impossible task, although there are clear indications of the best way to proceed.

There are several aspects to the aggregation of this data:

- Search mechanisms and strategies
- Document management and revisioning control
- Security and access control
- Single-point-of –access

Standard search methodologies will be ineffective for 'first pass' searches – these techniques are better deployed in refined search modalities. What is required is a spatial search engine that yields all available information about a specific location, as well as a capability to execute a proximity search for information within some geographic proximity to a specific location. An example might be a chemical refinery as a point location (with as-built drawings, diffusion studies and hydrant maps) and all transportation routes and residential housing within a 10 mile radius. Presenting such information visually, on one screen, to a decision maker provides a clear context for response.

One vital type of spatial search relates to the identification of exact location and status of all available responder units, together with a rough time-to-intercept calculation. This points to a requirement that any effective solution must be capable of dynamically accessing both real-time information as well as archival information.

Implicit in this is the system's capability to dynamically access many different databases in multiple locations. Such technology currently does exist although, once again, not in a productized and deployable form. This is a perfect example of a technology that could be productized for government application and then spun off into the private sector for cost recovery.

Once a spatial search is completed, a more refined search may then be initiated with standard technologies.

Document management technology should be mandatory to assure the key decision makers that the document they are depending on is the latest and most accurate. Security and access control should be an integral part of this application.

Finally, the ability of the decision makers to access all available information from a single access point is vital; jumping from terminal to terminal or relying on many subordinates to filter critical information during an engagement could lead to tremendous confusion.

3.2.4 Communications. The ability of the Ground Traffic controller to take action requires having access to multiple communications modalities; the operational need to access or initiate most of these modalities from a single console is readily apparent.

One point that must be made clear: the role of the Ground Traffic controller is to validate the existence of a credible threat and forward this information to authorized personnel. Ground traffic controllers should not be in the position of acting as Incident Command, which is the appropriate domain of the responder communities.

The types of communications range from voice (wireless and land-line) to text messaging and all forms of data transfer. Specific technologies are beyond the scope of this document.

The specific actions that a Ground Traffic controller will be required to undertake, and which will use one or more of the available communications modalities, include:

- Driver interrogation
- Remote vehicle shutdown
- GPS sensor interrogation
- Broadcast alerts to responder community
- Broadcast alerts to potential targets
- Request for data (database queries)
- Download active screen(s) of field operations to responder community (to establish an interactive field of view for Incident Command)

The majority of these actions are self-explanatory; however, the final item, downloading active screens, requires additional explanation. One of the key tasks of Ground Traffic Control is to aggregate as much relevant information as possible onto one console. Once this is achieved, the entire console can become virtual and downloaded to any location necessary. Furthermore, the requirement should be that the virtual console is downloaded fully functional as an operations center, with Ground Traffic Control now assuming an observer role. Fully functional implies that, in addition to displaying all of the aggregated information on a cartographic display, the virtual console must also maintain all of the communications capabilities that Ground Traffic Control had, as well as the ability to operate as a collaborative environment, allowing Incident Command to communicate directly with all deployed field personnel on any appropriate device.

What this means is that the Ground Traffic Control System must have, already embedded within its architecture, the capability of automatically transitioning into an Incident Command console from simply a Ground Traffic Control console. No operator action should be required; this transformation occurs any time a virtual console is downloaded to any Incident Command.

4.0 Summary

This paper advocates the immediate development and deployment of a Ground Traffic Control System for the purpose of tracking every hazardous materials shipment in the US.

The key components of such a system are:

- GPS tracking
- The Internet
- Cellular and satellite communications
- Cartographic software with database a searching and mining capability
- Geo-fencing software
- Analytic software for determining the existence of credible threats
- A database of potential targets
- Single-point-of-access display capability
- Virtual Console for Incident Command operations

From an operational perspective, an effective Ground Traffic Control System must be capable, at a minimum, of performing the following:

- Tracking the location, by asset class, of several million mobile objects in real-time
- Correlating each vehicle location with all nearby potential targets and responder assets

- Establishing the existence of a credible threat
- Notifying designated first responders
- Providing a collaborative environment for incident command operations

From a technology perspective, the system must:

- Provide cartographic displays with 'clickable' Points of Interest and drill down capability
- Have a user interface that can support multiple presentation layers, both as vector and raster information
- Be Internet based and use all applicable standards
- Have a highly scalable architecture
- Have response times that fall within any given time-to-intercept window for first responders
- Be capable of hosting and integrating the functionality of multiple third party applications
- Be capable of dynamically accessing multiple distributed databases
- Support thousands of end users simultaneously, despite different end user and access requirements
- Be easy to use with minimal learning curve
- Be capable of automatically transitioning from a tracking and monitoring environment into a collaborative operations environment

The core architecture to implement all of the foregoing currently exists, as do most of the requisite applications. Assembling and integrating all components into a single, fully operational Ground Traffic Control System can be accomplished relatively quickly, perhaps within 12 –18 months. The system could be built up in phases, with some key functionality coming on-line much faster. Full deployment, including the build-out of the regional Ground Traffic Control Centers should be accomplished within 2 – 3 years; once again, phasing-in key urban centers first could significantly reduce time to deployment in key areas.